

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-197058

(43)Date of publication of application : 19.07.2001

(51)Int.Cl.

H04L 12/24

H04L 12/26

H04L 12/56

(21)Application number : 2000-000496

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 05.01.2000

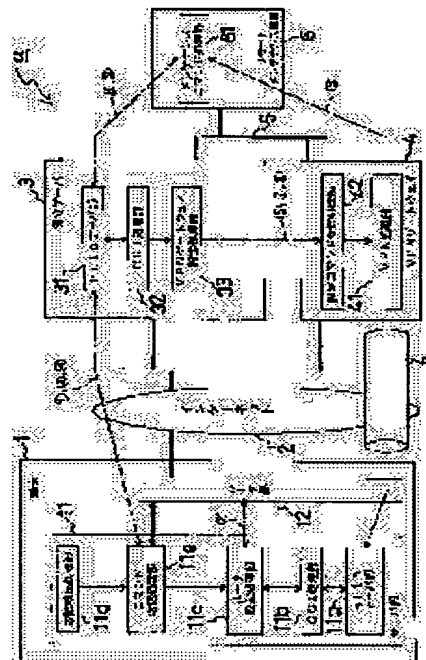
(72)Inventor : NAKAHAMA KIYOSHI  
YAMADA KEISHIN

## (54) METHOD FOR SHARING AUTHENTICATION KEY BETWEEN TERMINAL AND MAINTENANCE SERVER AND METHOD FOR TERMINAL REMOTE MAINTENANCE IMPLEMENTATION

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a terminal-maintenance server authentication key sharing method and a terminal remote maintenance implementing method which can remotely maintain a terminal by IPsec with high security without any operator's operation on the terminal side.

**SOLUTION:** After a terminal 1 is authenticated accompanying specific sharing authentication information as a fault of the terminal 1 is detected, a fault code and the global IP address of the terminal 1 are sent to the maintenance server 3, the setting of an authentication key of IPsec and the initiator setting of IPsec are written to a VPN gateway 4 controlled with commands from the maintenance server 3, and then necessary remote maintenance is carried out for a server part 11 and a router part 12 of the terminal 1 through a VPN tunnel set between the terminal 1 and maintenance server 3 (VPN gateway 4).



## LEGAL STATUS

[Date of request for examination] 27.11.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2001-197058  
(P2001-197058A)

(43)公開日 平成13年7月19日(2001.7.19)

(51)Int.Cl.<sup>7</sup>

H 0 4 L 12/24  
12/26  
12/56

識別記号

F I

H 0 4 L 11/08  
11/20

テーマコード(参考)

5 K 0 3 0  
1 0 2 Z

審査請求 未請求 請求項の数15 O L (全 19 頁)

(21)出願番号 特願2000-496(P2000-496)

(22)出願日 平成12年1月5日(2000.1.5)

(71)出願人 000004226

日本電信電話株式会社  
東京都千代田区大手町二丁目3番1号

(72)発明者 中濱 清志

東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内

(72)発明者 山田 敬信

東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内

(74)代理人 100071113

弁理士 菅 隆彦

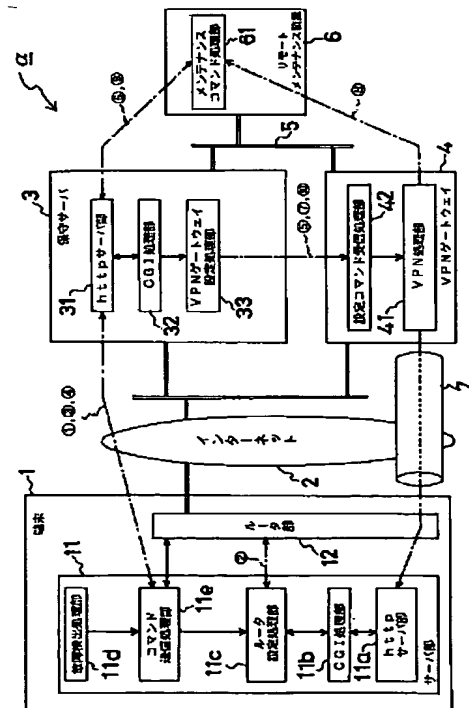
Fターム(参考) 5K030 GA15 HD03 JA10 JT02 LD19  
MA06 MB01

(54)【発明の名称】 端末-保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法

(57)【要約】

【課題】 I P s e cによる端末のリモートメンテナンスを、端末側における人間の操作なしにハイセキュリティに行うことの可能な端末-保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法の提供。

【解決手段】 端末1における故障検出に伴い、所定の共有認証情報に基づいて端末1の認証を行った後に、当該端末1の故障に係る故障コード及びグローバル I P アドレスを保守サーバ3へ送信すると共に、I P s e cの認証鍵の設定及びI P s e cのイニシエータ設定を、保守サーバ3からコマンド制御されるVPNゲートウェイ4に書き込み、これにより、端末1と保守サーバ3(VPNゲートウェイ4)との間に設定されるVPNトンネル7を通じ、端末1のサーバ部11及びルータ部12に対し所要のリモートメンテナンスを実施する特徴。



## 【特許請求の範囲】

【請求項 1】 インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、OS I 参照モデルのネットワーク層においてVPNセッションを実現するIPsecの認証鍵を共有するに当り、前記端末の設置時に、当該端末と前記保守サーバとで事前に共有される第 1 の共有認証情報に基づいて前記保守サーバ内で前記端末の認証を行い、この認証が成功した場合に、当該保守サーバ内で前記IPsecの認証鍵及び第 2 の共有認証情報をランダムに生成すると共に、これら生成した認証鍵及び第 2 の共有認証情報を、公開鍵暗号方式を用いて前記端末へ受け渡す設置通知処理と、該設置通知処理の完了に伴い、前記保守サーバから前記端末へ受け渡された前記認証鍵の設定を、当該端末のルータ部に書き込む端末VPN鍵設定処理と、を実行する、

ことを特徴とする端末－保守サーバ間認証鍵共有方法。

【請求項 2】 前記設置通知処理は、

前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末IDにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記第 1 の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、

前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記第 1 の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、

前記端末への前記認証鍵及び第 2 の共有認証情報の受渡しに先立ち、

前記端末内で生成した前記公開鍵暗号方式の公開鍵を前記保守サーバへ送信する処理と、

前記端末への前記認証鍵及び第 2 の共有認証情報の受渡しに際し、

前記端末から受信した前記公開鍵を用いて当該認証鍵及び第 2 の共有認証情報を暗号化し、これら暗号化後の認証鍵及び第 2 の共有認証情報を前記端末へ送信する処理と、

前記保守サーバから受信した当該暗号化後の認証鍵及び第 2 の共有認証情報を、前記端末内で前記公開鍵と共に生成した前記公開鍵暗号方式の秘密鍵を用いて復号化する処理と、を含む、

ことを特徴とする請求項 1 に記載の端末－保守サーバ間認証鍵共有方法。

【請求項 3】 前記端末VPN鍵設定処理は、

前記認証鍵の設定の前記端末のルータ部への書き込みの際、前記保守サーバからコマンド制御されるVPNゲートウェイを前記IPsecの対象ホストとする処理を含む、

ことを特徴とする請求項 1 又は 2 に記載の端末－保守サ

ーバ間認証鍵共有方法。

【請求項 4】 インターネットに端末型ダイヤルアップ接続された複数の端末を、OS I 参照モデルのネットワーク層においてVPNセッションを実現するIPsecにより、単一の保守サーバからリモートメンテナンスするに当り、

前記端末における故障の検出時に、当該端末と前記保守サーバとで事前に共有される所定の共有認証情報に基づいて、前記保守サーバ内で前記端末の認証を行うと共に、当該端末の故障に係る故障コードを前記保守サーバへ送信する故障通知処理と、

該故障通知処理の完了に伴い、前記所定の共有認証情報に基づいて、前記保守サーバにおいて前記端末の認証を行うと共に、前記端末型ダイヤルアップ接続に伴って前記端末のルータ部に設定されたグローバルIPアドレスを前記保守サーバへ送信するリモートメンテナンス要求処理と、

該リモートメンテナンス要求処理の完了に伴い、前記端末と前記保守サーバとで事前に共有される前記IPsecの認証鍵の設定、及び前記グローバルIPアドレスにより特定される前記IPsecのイニシエータ設定とを、前記保守サーバからコマンド制御されるVPNゲートウェイに書き込むVPNゲートウェイ設定処理と、該VPNゲートウェイ設定処理の完了に伴い、前記保守サーバからのコマンド制御に応じて、前記端末と前記保守サーバとの間に所要の前記VPNセッションを設定するVPNセッション開始指示処理と、

該VPNセッション開始指示の完了に伴い、前記故障コードの種別に応じた復旧指示コマンドの外部入力を受け付け、当該復旧指示コマンドの入力と共に、前記端末及び該端末のルータ部に対し所要の前記リモートメンテナンスを実施するリモートメンテナンス処理と、を実行する、

ことを特徴とする端末リモートメンテナンス実施方法。

【請求項 5】 前記故障通知処理は、

前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末IDにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、

前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、

前記端末から受信した前記故障コードを前記保守サーバ内に保持する処理と、を含む、

ことを特徴とする請求項 4 に記載の端末リモートメンテナンス実施方法。

【請求項 6】 前記リモートメンテナンス要求処理は、

## 3

前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末IDにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、

前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するかどうかを判別する処理と、

前記端末から受信した前記グローバルIPアドレスを前記保守サーバ内に保持する処理と、を含む、ことを特徴とする請求項4又は5に記載の端末リモートメンテナンス実施方法。

【請求項7】前記VPNゲートウェイ設定処理は、前記IPsecの認証鍵の設定及び同IPsecのインシエータ設定の書き込みの際し、前記端末のルータ部を前記IPsecの対象ホストとする処理を含む、ことを特徴とする請求項4、5又は6に記載の端末リモートメンテナンス実施方法。

【請求項8】前記VPNセッション開始指示処理は、前記VPNセッションの設定に際し、前記VPNゲートウェイと前記端末のルータ部との間に前記IPsecを確立する処理を含む、ことを特徴とする請求項4、5、6又は7に記載の端末リモートメンテナンス実施方法。

【請求項9】前記リモートメンテナンス処理は、前記リモートメンテナンスの実施に際し、前記復旧指示コマンドの入力を前記VPNゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記端末及び該端末のルータ部へ送信する処理を含む、ことを特徴とする請求項4、5、6、7又は8に記載の端末リモートメンテナンス実施方法。

【請求項10】前記VPNゲートウェイ設定処理と、前記VPNセッション開始指示処理の実行前は、それら処理間に、さらに前記リモートメンテナンスの開始指示に係る開始指示コマンドの外部入力を受け付け、当該開始指示コマンドの入力と共に、前記保守サーバに対し前記VPNセッションの設定開始に係る指示を与えるリモートメンテナンス開始指示処理を実行する、ことを特徴とする請求項4、5、6、7、8又は9に記載の端末リモートメンテナンス実施方法。

【請求項11】前記リモートメンテナンス開始指示処理は、前記リモートメンテナンスの開始指示に際し、前記開始指示コマンドの入力を前記VPNゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含む、

## 4

ことを特徴とする請求項10に記載の端末リモートメンテナンス実施方法。

【請求項12】前記リモートメンテナンス処理は、その完了後に、さらに前記リモートメンテナンスの終了指示に係る終了指示コマンドの外部入力を受け付け、当該終了指示コマンドの入力と共に、前記保守サーバに対し前記VPNセッションの設定終了に係る指示を与えるリモートメンテナンス終了指示処理と、

10 該リモートメンテナンス終了指示処理の完了に伴い、前記VPNゲートウェイに書き込まれていた前記IPsecの認証鍵の設定及び同IPsecのインシエータ設定を共に解除するVPNセッション終了指示処理と、を実行する、

ことを特徴とする請求項4、5、6、7、8、9、10又は11に記載の端末リモートメンテナンス実施方法。

【請求項13】前記リモートメンテナンス終了指示処理は、

前記リモートメンテナンスの終了指示に際し、前記終了指示コマンドの入力を前記VPNゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含む、

20 ことを特徴とする請求項12に記載の端末リモートメンテナンス実施方法。

【請求項14】前記VPNセッション終了指示処理は、前記IPsecの認証鍵の設定及び同IPsecのインシエータ設定の解除に際し、前記IPsecの対象ホストとされていた前記端末のルータ部における各対応設定を解除する処理を含む、

30 ことを特徴とする請求項12又は13に記載の端末リモートメンテナンス実施方法。

【請求項15】前記IPsecの認証鍵、及び前記所定の共有認証情報は、それぞれ、

請求項1、2又は3に記載の端末-保守サーバ間認証鍵共有方法において前記端末と前記保守サーバとで共有される前記認証鍵、及び前記第2の共有認証情報を適用する、

ことを特徴とする請求項4、5、6、7、8、9、10、11、12、13又は14に記載の端末リモートメンテナンス実施方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、端末-保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法に係わり、詳しくは、インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、OSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecの認証鍵を共有するための端末-保守サーバ間認証鍵共有方法、及びそれら複数の端末を、上記IPsecにより実際に単一の保守

サーバからリモートメンテナンスするための端末リモートメンテナンス実施方法に関する。

#### 【0002】

【従来の技術】一般に、インターネットに端末型ダイヤルアップ接続された複数の端末を単一の保守サーバにより一元的に管理し、それら端末に故障が発生した際にメンテナンスを実施する場合、その第1の方法として、故障が発生した端末から保守サーバに対しインターネット経由で故障通知を自動的に送信し、これを確認した保守サーバの管理者が派遣修理を行うか、又は、当該管理者からの電話指示等により端末の所有者自身が修理を行う方法が採られており、所要のメンテナンスを保守サーバからリモートで実施することは行われていなかった。

【0003】その主な理由としては、この第1の方法の場合、故障通知自体はダイヤルアップ接続により自動的に行われるものの、その故障通知後は、通常、端末内の無通信タイマにより短時間のうちに回線が切断されてしまい、リモートメンテナンスを実施しようとも、当該端末がインターネットにダイヤルアップ接続されているとは限らないためである。

【0004】また、たとえ端末がダイヤルアップ接続されていたとしても、通常では、当該端末のIPアドレスを知ることができないため、保守サーバ側からの接続は不可能であり、仮に、そのIPアドレスを知ることができたとしても、インターネット経由でメンテナンスを実施するのは、ローカルネットワーク上のメンテナンスと比較してセキュリティ上の問題がある（例えば、ローカルメンテナンス用のツールをそのまま転用すると、各種秘密情報がインターネット上に漏洩するおそれがある）。

【0005】こうした問題を解決するための第2の方法として、例えば、端末にリモートアクセスサーバ機能を具備させておき、故障通知後に、保守サーバの側から端末へ直接的に（インターネットを経由せずに）ダイヤルアップ接続を行い、さらに、コールバック等でセキュリティを確保した上で、所要のリモートメンテナンスを実施する方法が考えられる。

【0006】しかし、この第2の方法では、故障通知を発した端末が保守サーバの設置場所から遠隔地にある場合、ダイヤルアップ接続にかかる通信コストが自ずと高くなり、加えて、端末にダイヤルアップ接続の着信を許容すると、当該端末及び該端末の内部ネットワークのセキュリティが著しく低下するなどの問題を生じる。

【0007】このような問題に対処するため、第3の方法として、故障通知に伴い、端末の側からインターネット（プロバイダ）へダイヤルアップ接続し、OS参照モデルのネットワーク層においてアプリケーションに依存しない暗号通信を提供するIPsec等のプロトコルにより、インターネットに接続された任意のリモートメンテナンス装置との間でVPNセッションを設定し、当

該VPNセッション上で、所要のリモートメンテナンスを実施する方法なども考えられる。

【0008】このIPsecによるVPNセッションの確立は、認証鍵（Presharedkey）の交換と、IPsecプロトコルの1対1のグローバルIPアドレス通信とが可能であれば、技術的に何ら問題なく実現できる。

【0009】ここで、端末型ダイヤルアップ接続によりVPNセッションを確立し、所要のリモートメンテナンスを実施するための具体的手法を考察すれば、1）端末とVPNゲートウェイとで認証鍵を共有、2）端末を端末型ダイヤルアップ接続によりインターネットプロバイダ経由でインターネットに接続、3）端末に割り当てられたグローバルIPアドレスを確認、4）回線切断前にVPNゲートウェイの管理者にグローバルIPアドレスを連絡、5）双方で認証鍵交換の設定、6）双方でトンネルの設定、7）VPNによる通信／接続の確認、8）リモートメンテナンス処理を開始、9）リモートメンテナンスを運用（実施）、10）リモートメンテナンス処理を終了、11）双方でトンネルの設定を解除、12）双方で認証鍵交換の設定を解除、13）接続を終了、といった手順が必要となる。

#### 【0010】

【発明が解決しようとする課題】ここで、端末のリモートメンテナンスを実施するには、上述した第3の方法を人間の操作を介在させずに行えることが理想である。

【0011】しかしながら、上述もしたように、端末型ダイヤルアップ接続では、IPアドレスは固定されないのが一般的なため、その都度、人間の操作でIPアドレス関連の設定を変更する必要があり、実際のメンテナンスの運用を無人で行うことは事実上不可能である。

【0012】また、上述の認証鍵（Presharedkey）を2拠点のセキュリティゲートウェイ間で共有するには、それを紙面又は口頭で交換する必要があるなど、この場合にも人間の操作が介在し、IPsecの運用が極めて煩雑なものになる。

【0013】ここにおいて、本発明の解決すべき主要な目的は、次のとおりである。

【0014】即ち、本発明の第1の目的は、IPsecによる端末のリモートメンテナンスを、端末側における人間の操作なしにハイセキュリティに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法を提供せんとするものである。

【0015】本発明の第2の目的は、IPsecの確立を、人間の操作を介在させずに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法を提供せんとするものである。

【0016】本発明の第3の目的は、2拠点のセキュリティゲートウェイにおける認証鍵の共有を、人間の操作を介在させずに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法を

提供せんとするものである。

【0017】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0018】

【課題を解決するための手段】本発明端末—保守サーバ間認証鍵共有方法においては、端末の設置時に、当該端末と保守サーバとで事前に共有される第1の共有認証情報に基づいて保守サーバ内で端末の認証を行った後に、当該保守サーバ内でIPsecの認証鍵及び第2の共有認証情報をランダムに生成し、これら認証鍵及び第2の共有認証情報を公開鍵暗号方式を用いて端末へ受け渡し、保守サーバから端末へ受け渡された認証鍵の設定を当該端末のルータ部に書き込む、という特徴を有する。

【0019】本発明端末リモートメンテナンス実施方法においては、端末における故障検出に伴い、所定の共有認証情報に基づいて端末の認証を行った後に、当該端末の故障に係る故障コード及びグローバルIPアドレスを保守サーバへ送信すると共に、IPsecの認証鍵の設定及びIPsecのインシエータ設定を、保守サーバからコマンド制御されるVPNゲートウェイに書き込み、これにより、端末と保守サーバとの間に設定されるVPNセッション（VPNトンネル）を通じて、端末及び該端末のルータ部に対し所要のリモートメンテナンスを実施する、という特徴を有する。

【0020】さらに具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する新規な特徴的構成手法を採用することにより、前記目的を達成するよう為される。

【0021】即ち、本発明端末—保守サーバ間認証鍵共有方法の第1の特徴は、インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、OSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecの認証鍵を共有するに当り、前記端末の設置時に、当該端末と前記保守サーバとで事前に共有される第1の共有認証情報に基づいて前記保守サーバ内で前記端末の認証を行い、この認証が成功した場合に、当該保守サーバ内で前記IPsecの認証鍵及び第2の共有認証情報をランダムに生成すると共に、これら生成した認証鍵及び第2の共有認証情報を、公開鍵暗号方式を用いて前記端末へ受け渡し設置通知処理と、該設置通知処理の完了に伴い、前記保守サーバから前記端末へ受け渡された前記認証鍵の設定を、当該端末のルータ部に書き込む端末VPN鍵設定処理とを実行してなる、端末—保守サーバ間認証鍵共有方法の構成採用にある。

【0022】本発明端末—保守サーバ間認証鍵共有方法の第2の特徴は、上記本発明端末—保守サーバ間認証鍵共有方法の第1の特徴における前記設置通知処理が、前記保守サーバ内での前記端末の認証に先立ち、ユニーク

な端末IDにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記第1の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記第1の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、前記端末への前記認証鍵及び第2の共有認証情報の受渡しに先立ち、前記端末内で生成した前記公開鍵暗号方式の公開鍵を前記保守サーバへ送信する処理と、前記端末への前記認証鍵及び第2の共有認証情報の受渡しに際し、前記端末から受信した前記公開鍵を用いて当該認証鍵及び第2の共有認証情報を暗号化し、これら暗号化後の認証鍵及び第2の共有認証情報を前記端末へ送信する処理と、前記保守サーバから受信した当該暗号化後の認証鍵及び第2の共有認証情報を、前記端末内で前記公開鍵と共に生成した前記公開鍵暗号方式の秘密鍵を用いて復号化する処理とを含んでなる、端末—保守サーバ間認証鍵共有方法の構成採用にある。

【0023】本発明端末—保守サーバ間認証鍵共有方法の第3の特徴は、上記本発明端末—保守サーバ間認証鍵共有方法の第1又は第2の特徴における前記端末VPN鍵設定処理が、前記認証鍵の設定の前記端末のルータ部への書き込みの際に、前記保守サーバからコマンド制御されるVPNゲートウェイを前記IPsecの対象ホストとする処理を含んでなる、端末—保守サーバ間認証鍵共有方法の構成採用にある。

【0024】また、本発明端末リモートメンテナンス実施方法の第1の特徴は、インターネットに端末型ダイヤルアップ接続された複数の端末を、OSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecにより、単一の保守サーバからリモートメンテナンスするに当り、前記端末における故障の検出時に、当該端末と前記保守サーバとで事前に共有される所定の共有認証情報に基づいて、前記保守サーバ内で前記端末の認証を行うと共に、当該端末の故障に係る故障コードを前記保守サーバへ送信する故障通知処理と、該故障通知処理の完了に伴い、前記所定の共有認証情報に基づいて、前記保守サーバにおいて前記端末の認証を行うと共に、前記端末型ダイヤルアップ接続に伴って前記端末のルータ部に設定されたグローバルIPアドレスを前記保守サーバへ送信するリモートメンテナンス要求処理と、該リモートメンテナンス要求処理の完了に伴い、前記端末と前記保守サーバとで事前に共有される前記IPsecの認証鍵の設定、及び前記グローバルIPアドレスにより特定される前記IPsecのインシエータ設定とを、前記保守サーバからコマンド制御されるVPNゲートウェイに書き込むVPNゲートウェイ設定処理と、該VPNゲートウェイ設定処理の完了に伴い、前記保守サ

サーバからのコマンド制御に応じて、前記端末と前記保守サーバとの間に所要の前記VPNセッションを設定するVPNセッション開始指示処理と、該VPNセッション開始指示の完了に伴い、前記故障コードの種別に応じた復旧指示コマンドの外部入力を受け付け、当該復旧指示コマンドの入力と共に、前記端末及び該端末のルータ部に対し所要の前記リモートメンテナンスを実施するリモートメンテナンス処理とを実行してなる、端末リモートメンテナンス実施方法の構成採用にある。

【0025】本発明端末リモートメンテナンス実施方法の第2の特徴は、上記本発明端末リモートメンテナンス実施方法の第1の特徴における前記故障通知処理が、前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末IDにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、前記端末から受信した前記故障コードを前記保守サーバ内に保持する処理とを含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0026】本発明端末リモートメンテナンス実施方法の第3の特徴は、上記本発明端末リモートメンテナンス実施方法の第1又は第2の特徴における前記リモートメンテナンス要求処理が、前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末IDにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、前記端末から受信した前記グローバルIPアドレスを前記保守サーバ内に保持する処理とを含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0027】本発明端末リモートメンテナンス実施方法の第4の特徴は、上記本発明端末リモートメンテナンス実施方法の第1、第2又は第3の特徴における前記VPNゲートウェイ設定処理が、前記IPsecの認証鍵の設定及び同IPsecのインシエータ設定の書込みに際し、前記端末のルータ部を前記IPsecの対象ホストとする処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0028】さらに、本発明端末リモートメンテナンス実施方法の第5の特徴は、上記端末リモートメンテナン

ス実施方法の第1、第2、第3又は第4の特徴における前記VPNセッション開始指示処理が、前記VPNセッションの設定に際し、前記VPNゲートウェイと前記端末のルータ部との間に前記IPsecを確立する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0029】本発明端末リモートメンテナンス実施方法の第6の特徴は、上記端末リモートメンテナンス実施方法の第1、第2、第3、第4又は第5の特徴における前記リモートメンテナンス処理が、前記リモートメンテナンスの実施に際し、前記復旧指示コマンドの入力を前記VPNゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記端末及び該端末のルータ部へ送信する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0030】本発明端末リモートメンテナンス実施方法の第7の特徴は、上記端末リモートメンテナンス実施方法の第1、第2、第3、第4、第5又は第6の特徴における前記VPNゲートウェイ設定処理と、前記VPNセッション開始指示処理と、それら処理間に、さらに、前記リモートメンテナンスの開始指示に係る開始指示コマンドの外部入力を受け付け、当該開始指示コマンドの入力と共に、前記保守サーバに対し前記VPNセッションの設定開始に係る指示を与えるリモートメンテナンス開始指示処理を実行してなる、端末リモートメンテナンス実施方法の構成採用にある。

【0031】本発明端末リモートメンテナンス実施方法の第8の特徴は、上記端末リモートメンテナンス実施方法の第7の特徴における前記リモートメンテナンス開始指示処理が、前記リモートメンテナンスの開始指示に際し、前記開始指示コマンドの入力を前記VPNゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0032】本発明端末リモートメンテナンス実施方法の第9の特徴は、上記端末リモートメンテナンス実施方法の第1、第2、第3、第4、第5、第6、第7又は第8の特徴における前記リモートメンテナンス処理が、その完了後に、さらに、前記リモートメンテナンスの終了指示に係る終了指示コマンドの外部入力を受け付け、当該終了指示コマンドの入力と共に、前記保守サーバに対し前記VPNセッションの設定終了に係る指示を与えるリモートメンテナンス終了指示処理と、該リモートメンテナンス終了指示処理の完了に伴い、前記VPNゲートウェイに書き込まれていた前記IPsecの認証鍵の設定及び同IPsecのインシエータ設定を共に解除するVPNセッション終了指示処理とを実行してなる、端末リモートメンテナンス実施方法の構成採用にある。



【0033】本発明端末リモートメンテナンス実施方法の第10の特徴は、上記端末リモートメンテナンス実施方法の第9の特徴における前記リモートメンテナンス終了指示処理が、前記リモートメンテナンスの終了指示に際し、前記終了指示コマンドの入力を前記VPNゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0034】本発明端末リモートメンテナンス実施方法の11の特徴は、上記端末リモートメンテナンス実施方法の第9又は第10の特徴における前記VPNセッション終了指示処理が、前記IPsecの認証鍵の設定及び同IPsecのイニシエータ設定の解除に際し、前記IPsecの対象ホストとされていた前記端末のルータ部における各対応設定を解除する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【0035】本発明端末リモートメンテナンス実施方法の第12の特徴は、上記端末リモートメンテナンス実施方法の第1、第2、第3、第4、第5、第6、第7、第8、第9、第10又は第11の特徴における前記IPsecの認証鍵、及び前記所定の共有認証情報に、それぞれ、請求項1、2又は3に記載の端末-保守サーバ間認証鍵共有方法において前記端末と前記保守サーバとで共有される前記認証鍵、及び前記第2の共有認証情報を適用してなる、端末リモートメンテナンス実施方法の構成採用にある。

#### 【0036】

【発明の実施の形態】以下、本発明の実施の形態を、添付図面を参照しつつ、まず、本発明の適用を受ける適用システムの構成例につき説明し、次いで、当該適用システムにおいて実施される方法例につき説明する。

【0037】（適用システム構成例）図1は、本発明の適用システムであるリモートメンテナンスシステムの構成を示す図である。

【0038】同図に示すように、このリモートメンテナンスシステムαは、4つのノード、即ち、リモートメンテナンスの対象となる端末1と、この端末1にインターネット2を経由して接続される保守サーバ3と、この保守サーバ3からコマンド制御されるVPNゲートウェイ4と、このVPNゲートウェイ4にLAN等のローカルネットワーク5で接続されたリモートメンテナンス装置

6とを有して構成される。また、端末1と保守サーバ3との間には、VPNゲートウェイ4を経由してVPNトンネル7が設定される。

【0039】端末1は、本発明における故障検出機能及び復旧機能を実現するサーバ部11と、IPsecを含んだIPルータ処理を制御するルータ部12とを有して構成され、このうちのサーバ部11は、さらに、httpサーバ処理を行うhttpサーバ部11aと、このhttpサーバ部11aからコールされて内部処理を行うCGI処理部11bと、ルータ部12への制御コマンドを発行するルータ設定処理部11cと、端末1及びルータ部12の故障を検出する故障検出処理部11dと、保守サーバ3に所要のコマンドを送信するコマンド送信処理部11eとを有して構成される。

【0040】保守サーバ3は、端末1から送信されるhttpコマンドを受信するhttpサーバ部31と、このhttpサーバ部31からコールされて内部処理を行うCGI処理部32と、VPNゲートウェイ4へtelnetコマンドを発行するVPNゲートウェイ設定処理部33とを有して構成される。

【0041】VPNゲートウェイ4は、端末1のルータ部12との間でVPNセッションを行うVPN処理部41と、保守サーバ3のVPNゲートウェイ設定処理部33から送信されるtelnetコマンドを受信する設定コマンド受信処理部42とを有して構成される。

【0042】リモートメンテナンス装置6は、端末1のサーバ部11に対し、httpコマンド等によりコマンドを送信するメンテナンスコマンド処理部61を有して構成される。

【0043】なお、以上のリモートメンテナンスシステムαは、その説明からも明らかなように、各ノード間の通信プロトコルとして、httpやtelnetを適用することを前提としたものだが、各処理部間の通信が円滑に行えれば、その通信プロトコルの種別は特に問うものではない。但し、本発明では、インターネット間の通信を前提としているため、TCP/IP上の通信プロトコルであることは必須である（汎用性を考慮すると、httpからCGIを起動する形態であることが望ましい）。

【0044】

【外1】

13

ここで、図示の①～⑩は、本発明において実行される各処理の通信データ（コマンド送信及び受信）のルートを示しており、それぞれ、①は「設置通知処理」の、②は「端末VPN鍵設定処理」の、③は「故障通知処理」の、④は「リモートメンテナンス要求処理」の、⑤は「VPNゲートウェイ設定処理」の、⑥は「リモートメンテナンス開始指示処理」の、⑦は「VPNセッション開始指示処理」の、⑧は「リモートメンテナンス処理」の、⑨は「リモートメンテナンス終了指示処理」、⑩は「VPNセッション終了指示処理」の通信データのルートである。

14

【0045】このうち、及びの処理は、本発明にお 10 だけ実行される。

ける端末－保守サーバ間認証鍵共有方法を実現するため

【0046】

の処理であり、これらの処理は、端末1の設置時に一度

【外2】

また、残る③～⑩の処理は、本発明における端末リモートメンテナンス実施方法を実現するための処理であり、これら一連の処理は、リモートメンテナンスの実施が要求されるごとに実行される。このうち、リモートメンテナンス装置6から起動される⑥、⑧及び⑨の処理については、人間の操作が必要とされるが、その他の端末1側からの処理は、当該端末1における故障発生を検出を受け、各処理が連携しながら自動的に起動される。

【0047】なお、本発明の実施に際しては、以下に示す前提条件が必要とされる。

【0048】（1）（複数の）端末1が、その出荷時において個々にユニークな端末IDを持つこと。

【0049】（2）端末1と保守サーバ3が、本発明にいう第1の共有認証情報を事前に共有していること（以下、第1の共有認証情報を、「Secret(id)」とも表記する。「id」は、端末IDと同一の値であり、従って、Secret(id)は、端末IDごとにユニークな共有秘密情報である）。なお、Secret(id)は、端末1の出荷時に、当該端末1内のROM等に埋め込み、保守サーバ3と共有することで対応する（当該Secret(id)は、保守サーバ3がリモートメンテナンスを行う全ての端末1で共通であってもよい）。

【0050】（3）端末1のルータ部12が、IPsec等のIPレベルのVPN機能を持ち、また、VPNセッションについて、セッション待受け側の設定を事前に行っておくこと（IPsecの場合は、当該ルータ部12をレスポンドとして設定する）。なお、認証鍵（以下、「Presharedkey」とも表記する）にはダミーデータを設定しておくこと。

【0051】（4）VPNゲートウェイ4が、端末1のルータ部12と通信互換性のあるVPN機能を持つこと。

【0052】（5）端末1のルータ部12が、保守サーバ3の公開されたグローバルIPアドレス、又はこれと等価のインターネットホスト名を、の設置通知処理の時点までに事前に知っていること。また、インターネットへの接続手段として、端末型ダイヤルアップ接続を適用することとし、その設定が既に完了していること。

【0053】（6）端末1のサーバ部11におけるルー

20 タ設定処理部11cからルータ部12への各種通信設定が、リモートコンソール（以下、「telnet」という）又はプロセス間通信で行えること。

【0054】（7）保守サーバ3のVPNゲートウェイ設定処理部33からVPNゲートウェイ4の設定コマンド受信処理部42への各種通信設定が、telnetで行えること。

【0055】（8）の設置通知処理、の故障通知処理、及びのリモートメンテナンス要求処理におけるメッセージ認証子（以下、「MAC」とも表記する）の計算アルゴリズムが、端末1と保守サーバ3とで共通であること。（以上、実施前提条件）

【0056】（方法例）続いて、上述したリモートメンテナンスシステムαに適用される方法例について説明する。なお、本発明は、「端末－保守サーバ間認証鍵共有方法」と「端末リモートメンテナンス実施方法」とを包含するものであるが、両者は互いに密接な関係を有するため、本方法例においては、これらを特に区別することなく説明するものとする。

【0057】＜設置通知処理＞本設置通知処理は、端末1が設置されたことをリモートメンテナンスに先立って保守サーバ3へ通知し、その保守サーバ3から、本発明にいう第2の共有認証情報を受け取ることを目的とする（以下、第2の認証情報を、「Secret2(id)」とも表記する。「id」は、端末IDと同一の値であり、従って、Secret2(id)は、端末IDごとにユニークな共有秘密情報である）。なお、ここで、Secret(id)の代わりにSecret2(id)を用いるのは、端末1の全てに共通している可能性があるSecret(id)よりも、このSecret2(id)を用いた方が、セキュリティが強化されるためである。以下、図面により、本設置通知処理の詳細を説明する。

50

【0058】図2は、本発明の方法例に係る設置通知処理を説明するためのフローチャートである。

【0059】同図に示すように、本設置通知処理は、端末1の設置終了後（ST1）、インターネット2への接続設定が完了した時点で（ST2）、当該端末1の管理者（所有者）の操作により、サーバ部11において一度だけ実行される。

【0060】即ち、サーバ部11は、そのコマンド送信処理部11eにおいて、まず、公開鍵暗号化方式のアルゴリズム（RSA等）により、秘密鍵及び公開鍵を生成すると共に（ST3）、端末IDに現在のタイムスタンプを付加してなる原文を作成し（ST4）、さらに、この原文に対し、端末1内に事前に設定されたSecret(id)を用いてメッセージ認証子（MAC）を生成する（ST5）。なお、このメッセージ認証子の生成に際しては、ISO9797-1及びISO9797-2に準拠することが望ましい（以下、メッセージ認証子の生成について同じ）。

【0061】そして、コマンド送信処理部11eは、「設置通知を示すコード」、「端末ID」、「原文」、「MAC」、及び「公開鍵」をパラメータとしたhttpコマンドを、非IPsecセッションにより、保守サーバ3のhttpサーバ部31に向けて送信する（ST6）。

【0062】保守サーバ3のhttpサーバ部31では、端末1から送信された上記コマンドを受信し（ST7）、その受信に係るコマンド名及びパラメータをCGI処理部32へ受け渡す。

【0063】CGI処理部32は、上記パラメータ中の原文に対し、保守サーバ3内に事前に設定されたSecret(id)を用いてメッセージ認証子（MAC）を生成し（端末1におけるそれと同様の演算）、これが上記パラメータ中のMACと一致することを確認して、端末1の認証を行う（ST8）。

【0064】そして、CGI処理部32は、IPsecの認証鍵であるPresharedkeyとSecret2(id)とをランダムに生成し（ST9、ST10）、これらを、上記パラメータ中の端末IDに対応したデータとして自身に保持すると共に、同パラメータ中の暗号鍵で暗号化する（ST11）。

【0065】次に、保守サーバ3のhttpサーバ部31は、上記CGI処理部32から、端末1の認証に関する「ステータス（正常又はエラーステータス）」、「暗号化後のPresharedkey」、及び「暗号化後のSecret2(id)」を取得し、これらをパラメータとしたhttpレスポンスを、非IPsecセッションにより、端末1のサーバ部11におけるコマンド送信処理部11eに向けて送信する（ST12）。

【0066】そして、端末1のサーバ部11におけるコマンド送信処理部11eは、保守サーバ3から送信され

た上記レスポンスを受信し（ST13）、これに含まれるパラメータ中の暗号化後のPresharedkey及び同Secret2(id)を、それぞれ先に生成しておいた秘密鍵で復号化して自身に保持し（ST14、ST15）、処理の端末VPN鍵設定処理へと受け渡す（図示の記号「A」により連続）。

【0067】なお、端末1の後処理として、これ以降に用いられることのないSecret(id)を消去すれば、よりセキュリティが強まるが、これは必須ではない。

10 【0068】＜ 端末VPN鍵設定処理＞本端末VPN鍵設定処理は、上述の設置通知処理の完了後、端末1のルータ部12に対しPresharedkeyを設定することを目的とする。以下、図面により、本端末VPN鍵設定処理の詳細を説明する。

【0069】図3は、本発明の方法例に係る端末VPN鍵設定処理を説明するためのフローチャートである。

20 【0070】同図に示すように、本端末VPN鍵設定処理は、上述の設置通知処理の完了を契機（A）に開始される。即ち、端末1のサーバ部11におけるルータ設定処理部11cは、Presharedkeyの取得に伴い（ST16）、まず、VPNゲートウェイ4をIPsecの対象ホストとした「Presharedkeyの設定（ルータ部12のtelnetコマンドの実装形態により異なる）」をパラメータとしたtelnetコマンドを、ローカルネットワークセッションにより、同端末1のルータ部12に向けて送信する（ST17）。

30 【0071】ルータ部12は、サーバ部11から送信された上記コマンドを受信し（ST18）、その受信に係るコマンド中のパラメータであるPresharedkeyの設定を自身に書き込み（ST19）、さらに、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとしたtelnetレスポンスを、ローカルネットワークセッションにより、同端末1のサーバ部11におけるルータ設定処理部11cに向けて送信し（ST20）、所要のVPN設定を完了する。

40 【0072】そして、端末1のサーバ部11におけるルータ設定処理部11cは、ルータ部12から送信された上記レスポンスを受信し（ST21）、以上により、所要の端末1の設置に係る全ての処理（の設置通知処理、及びの端末VPN鍵設定処理）を完了する。

【0073】＜ 故障通知処理＞本故障通知処理は、端末1のサーバ部11及びルータ部12に故障が発生したことを随時に検出し、その状態を保守サーバ3に通知することを目的とする。以下、図面により、本故障通知処理の詳細を説明する。

【0074】図4は、本発明の方法例に係る故障通知処理を説明するためのフローチャートである。

50 【0075】同図に示すように、本故障通知処理は、端末1のサーバ部11における故障検出処理部11dが、同端末1のサーバ部11及びルータ部12に故障が発生

したことを検出した時点で開始される（ST31）。即ち、この故障検出処理部11dは、サーバ部11及びルータ部12における故障の発生及び復旧の状態を常時監視し、何らかの故障が発生した時点で、本故障通知処理を起動する。

【0076】端末1に故障が検出されると、同端末1のサーバ部11におけるコマンド送信処理部11eは、まず、端末IDに現在のタイムスタンプを付加してなる原文を作成し（ST32）、さらに、この原文に対し、端末1内に新たに設定されたSecret2(id)を用いてメッセージ認証子（MAC）を生成する（ST33）。

【0077】そして、コマンド送信処理部11eは、「故障通知を示すコード」、「端末ID」、「原文」、「MAC」、及び「故障コード」をパラメータとしたhttpコマンドを、非IPsecセッションにより、保守サーバ3のhttpサーバ部31に向けて送信する（ST34）。

【0078】保守サーバ3のhttpサーバ部31では、端末1から送信された上記コマンドを受信し（ST35）、その受信に係るコマンド名及びパラメータをCGI処理部32へ受け渡す。

【0079】CGI処理部32は、上記パラメータ中の原文に対し、保守サーバ3内に新たに設定されたSecret2(id)を用いてメッセージ認証子（MAC）を生成し（端末1におけるそれと同様の演算）、これが上記パラメータ中のMACと一致することを確認して、端末1の認証を行い（ST36）、さらに、上記パラメータ中の故障コードを、同パラメータ中の端末IDに対応したデータとして自身に保持する（ST37）。

【0080】次に、保守サーバ3のhttpサーバ部31は、上記CGI処理部32から、端末1の認証に関する「ステータス（正常又はエラーステータス）」を取得し、当該ステータスをパラメータとしたhttpレスポンスを、非IPsecセッションにより、端末1のサーバ部11におけるコマンド送信処理部11eに向けて送信する（ST38）。

【0081】そして、端末1のサーバ部11におけるコマンド送信処理部11eは、保守サーバ3から送信された上記レスポンスを受信し（ST39）、以上により、この故障通知処理を完了して、処理をのリモートメンテナンス要求処理へと受け渡す（図示の記号「B」により連続）。

【0082】なお、本故障通知処理において、端末IDに対応したデータとして保持した故障コードは、端末1における故障状態の確認のため、リモートメンテナンス装置6からhttpアクセス等により参照できることが望ましい。

【0083】＜リモートメンテナンス要求処理＞本リモートメンテナンス要求処理は、上述の故障通知処理と連動して、IPsecによるリモートメンテナンスの実

施を保守サーバ3に要求することを目的とする。但し、故障通知処理と連動したリモートメンテナンスが速やかに行われない場合は、インターネット2との接続が切断されて、確立したVPNトンネル7が消失する可能性があるため、端末1の管理者が、当該リモートメンテナンス要求処理を手動操作で立ち上げることも併せて許容する。以下、図面により、本リモートメンテナンス要求処理の詳細を説明する。

【0084】図5は、本発明の方法例に係るリモートメンテナンス要求処理及びVPNゲートウェイ設定処理を説明するためのフローチャートである。

【0085】同図に示すように、本リモートメンテナンス要求処理は、上述の故障通知処理の完了を契機（B）に、又は、端末1の管理者のボタン操作等による当該端末1へのアクション（ST40）に応じて開始される。即ち、端末1のサーバ部11におけるコマンド送信処理部11eは、まず、端末1がインターネット2に接続されているか否かを判別し（ST41）、それが未だ接続されていない場合には（ST41；N）、インターネット2に接続した後に（ST42）、既に接続されている場合には（ST41；Y）、直ちに、端末IDに現在のタイムスタンプを付加してなる原文を作成し（ST43）、さらに、この原文に対し、端末1内に設定されたSecret2(id)を用いてメッセージ認証子（MAC）を生成する（ST44）。

【0086】そして、コマンド送信処理部11eは、端末1のルータ部12から、ダイヤルアップ接続時にインターネットプロバイダからIPCPで割り当てられた、当該ルータ部12のグローバルIPアドレスを取得し（ST45）、さらに、「リモートメンテナンス要求を示すコード」、「端末ID」、「原文」、「MAC」、及び「グローバルIPアドレス」をパラメータとしたhttpコマンドを、非IPsecセッションにより、保守サーバ3のhttpサーバ部31に向けて送信する（ST46）。

【0087】保守サーバ3のhttpサーバ部31では、端末1から送信された上記コマンドを受信し（ST47）、その受信に係るコマンド名及びパラメータをCGI処理部32へ受け渡す。

【0088】CGI処理部32は、上記パラメータ中の原文に対し、保守サーバ3内に設定されたSecret2(id)を用いてメッセージ認証子（MAC）を生成し（端末1におけるそれと同様の演算）、これが上記パラメータ中のMACと一致することを確認して、端末1の認証を行い（ST48）、さらに、上記パラメータ中のグローバルIPアドレス（以下、「ルータIPアドレス」という）を、同パラメータ中の端末IDに対応したデータとして自身に保持する（ST49）。

【0089】次に、保守サーバ3のhttpサーバ部31は、上記CGI処理部32から、端末1の認証に関する

る「ステータス（正常又はエラーステータス）」を取得し、当該ステータスをパラメータとした `http` レスポンスを、非 `IPsec` セッションにより、端末 1 のサーバ部 11 におけるコマンド送信処理部 11e に向けて送信する（ST50）。

【0090】そして、端末 1 のサーバ部 11 におけるコマンド送信処理部 11e は、保守サーバ 3 から送信された上記レスポンスを受信し（ST51）、以上により、このリモートメンテナンス要求処理を完了して、処理を

の VPN ゲートウェイ設定処理へと受け渡す。

【0091】＜VPNゲートウェイ設定処理＞本VPNゲートウェイ設定処理は、上述のリモートメンテナンス要求処理と連動して、保守サーバ 3 で受信されたルータ IP アドレスをもとに、VPNゲートウェイ 4 に対し、Presharedkey の設定及び `IPsec` イニシエータ設定の書き込みを行うことを目的とする。以下、前述の図 5 により、本VPNゲートウェイ設定処理の詳細を説明する。

【0092】同図に示すように、本VPNゲートウェイ設定処理は、上述のリモートメンテナンス要求処理における正常終了レスポンスの送信を契機（ST50のステップ）に開始される。即ち、保守サーバ 3 のVPNゲートウェイ設定処理部 33 は、まず、CGI 処理部 32 から、`IPsec` の認証鍵である Presharedkey とルータ IP アドレスとを取得して（ST52、ST53）、端末 1 のルータ部 12 をそれぞれ `IPsec` の対象ホストとした「Presharedkey の設定（VPNゲートウェイ 4 の `telnet` コマンドの実装形態により異なる）」、及び「`IPsec` イニシエータ設定（VPNゲートウェイ 4 の `telnet` コマンドの実装形態により異なる）」を

パラメータとした `telnet` コマンドを生成し（ST54）、当該コマンドを、ローカルネットワークセッションにより、VPNゲートウェイ 4 に向けて送信する（ST55）。

【0093】VPNゲートウェイ 4 は、その設定コマンド受信処理部 42 において、保守サーバ 3 から送信された上記コマンドを受信し（ST56）、その受信に係るコマンド中のパラメータである Presharedkey の設定と `IPsec` イニシエータの設定とを自身に書き込み（ST57）、さらに、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとした `telnet` レスポンスを、ローカルネットワークセッションにより、保守サーバ 3 のVPNゲートウェイ設定処理部 33 に向けて送信し（ST58）、所要のVPN設定を完了する。

【0094】そして、保守サーバ 3 のVPNゲートウェイ設定処理部 33 は、VPNゲートウェイ 4 から送信された上記レスポンスを受信し（ST59）、以上により、本VPNゲートウェイ設定処理を完了する。

【0095】なお、以上のVPN設定が完了した段階

で、その状態がリモートメンテナンス装置 6 から確認できることが望ましい。その理由は、VPN設定が完了したことを確認した上で、以降に続くのリモートメンテナンス開始指示処理を実行できた方が、リモートメンテナンスの実施者の作業効率が良いからである（リモートメンテナンス開始指示処理の成功する確率が高い）。

【0096】＜リモートメンテナンス開始指示処理＞本リモートメンテナンス開始指示処理は、リモートメンテナンス装置 6 を使用して、実際にリモートメンテナンスを開始することを保守サーバ 3 に伝えることを目的とする。以下、図面により、本リモートメンテナンス開始指示処理の詳細を説明する。

【0097】図 6 は、本発明の方法例に係るリモートメンテナンス開始指示処理を説明するためのフローチャートである。

【0098】同図に示すように、本リモートメンテナンス開始指示処理は、リモートメンテナンスの実施者の手動操作により開始される。即ち、リモートメンテナンス装置 6 のメンテナンスコマンド処理部 61 は、「リモートメンテナンス開始を示すコード」をパラメータとした `http` コマンドを、ローカルネットワークセッションにより、保守サーバ 3 の `http` サーバ部 31 に向け送信する（ST60）。

【0099】保守サーバ 3 の `http` サーバ部 31 では、リモートメンテナンス装置 6 から送信された上記コマンドを受信し（ST61）、以下、処理を

の VPN セッション開始指示処理へと受け渡す（図示の記号「C」により連続）。

【0100】なお、本リモートメンテナンス開始指示処理は、実際には、以降に続くVPNセッション開始指示処理が完了するまで起動状態を維持する。その詳細については、以下のVPNセッション開始指示処理で併せて説明する（図示の記号「D」により連続）。

【0101】＜VPNセッション開始指示処理＞本VPNセッション開始指示処理は、上述のリモートメンテナンス開始指示処理の内部処理として機能し、リモートメンテナンスの開始指示に引き続き、`IPsec` セッションを確立することを目的とする。以下、図面により、本VPNセッション開始指示処理の詳細を説明する。

【0102】図 7 は、本発明の方法例に係るVPNセッション開始指示処理を説明するためのフローチャートである（一部、リモートメンテナンス開始指示処理を含む）。

【0103】同図に示すように、本VPNセッション開始指示処理は、上述のリモートメンテナンス開始処理による起動を契機（C）に開始される。即ち、保守サーバ 3 のVPNゲートウェイ設定処理部 33 は、まず、端末 1 のルータ部 12 を `IPsec` の対象ホストとした「`IPsec` セッションの開始設定（VPNゲートウェイ 4 の `telnet` コマンドの実装形態により異なる）」を

パラメータとした `telnet` コマンドを、ローカルネットワークセッションにより、VPNゲートウェイ4に向けて送信する (ST62)。

【0104】VPNゲートウェイ4は、その設定コマンド受信処理部42において、保守サーバ3から送信された上記コマンドを受信して (ST63)、当該コマンドをVPN処理部41へ受け渡し、さらに、このVPN処理部41において、端末1のルータ部12との間でIPsecを相互に確立する処理を実行して (ST64、ST65)、所要のIPsecのリンクを確立する (ST66)。

【0105】次に、以上のIPsecの確立に伴い、VPNゲートウェイ4の設定コマンド受信処理部42は、上記コマンドに対する「ステータス (正常又はエラーステータス)」をパラメータとした `telnet` レスポンスを、ローカルネットワークセッションにより、保守サーバ3のVPNゲートウェイ設定処理部33に向けて送信する (ST67)。

【0106】そして、保守サーバ3のVPNゲートウェイ設定処理部33は、VPNゲートウェイ4から送信された上記レスポンスを受信し (ST68)、以上により、このVPNセッション開始指示処理を完了して、処理をのリモートメンテナンス開始指示処理へと引き戻す。

【0107】ここで、リモートメンテナンス開始指示処理は、上述のVPNセッション開始指示処理における正常又は異常レスポンスの受信を契機 (ST68のステップ) に開始される。即ち、保守サーバ3の `http` サーバ部31は、上記レスポンスに対する「ステータス (IPsec確立又はエラーステータス)」をパラメータとした `http` レスポンスを、ローカルネットワークセッションにより、リモートメンテナンス装置6のメンテナンスコマンド処理部61に向けて送信する (ST69)。

【0108】そして、リモートメンテナンス装置6のメンテナンスコマンド処理部61は、保守サーバ3から送信された上記レスポンスを受信し (ST70)、以上により、このVPNセッション開始指示処理を完了して、処理をのリモートメンテナンス処理へと受け渡す。

【0109】なお、リモートメンテナンス装置6の後処理として、保守サーバ3から正常なIPsec確立レスポンスが返送された場合には、後述するのリモートメンテナンス処理を実行し、これに対し、エラーレスポンスが返送された場合には、端末1がインターネット2に接続されていないものと判断して、前述したのリモートメンテナンス要求処理を再起動するよう、端末1の管理者に連絡することが必要である。

【0110】＜リモートメンテナンス処理＞本リモートメンテナンス処理は、暗号化された伝送路としてのIPsec等のVPNトンネル7を経由して、リモートメ

ンテナンス装置6からセキュアなリモートメンテナンスを実施し、端末1における故障を復旧することを目的とする。なお、ここで用いるリモートメンテナンス装置6は、特殊なものである必要はなく、ローカルネットワーク5上でコマンドを送信することにより、端末1をメンテナンスできる装置 (例えば、`http` クライアント (ウェブブラウザ) や `telnet` ツールなど) であれば、それを転用できる。また、その機能としては、ある故障 (例えば、Proxy故障) に関し、その復旧動作 (Proxyの起動、端末1の再起動) を行う機能の他、例えば、端末1のログ表示や、ルータ部12における各種設定の確認などを行う機能も具備する。以下、図面により、本リモートメンテナンス処理の詳細を説明する。

【0111】図8は、本発明の方法例に係るリモートメンテナンス処理を説明するためのフローチャートである。

【0112】同図に示すように、本リモートメンテナンス処理は、上述のリモートメンテナンス開始指示処理においてIPsec確立レスポンスが返送されて以降、端末1がインターネット2に接続しており、VPNトンネル7が設定されている状態において、リモートメンテナンスの実施者の手動操作により任意の契機で開始される。即ち、リモートメンテナンス装置6のメンテナンスコマンド処理部61は、「リモートメンテナンスコマンドであることを示すコード」、「リモートメンテナンスコマンド種別 (サーバ部11/ルータ部12)」、及び「リモートメンテナンスコマンド詳細パラメータ」をパラメータとした `http` コマンドを、VPNセッションにより (VPNトンネル7を通じ)、端末1のサーバ部11における `http` サーバ部11aに向け送信する (ST71)。

【0113】端末1のサーバ部11では、リモートメンテナンス装置6から送信された上記コマンドを受信し (ST72)、その受信に係るコマンド名及びパラメータを、まず、同端末1のCGI処理部11bへ受け渡す。

【0114】CGI処理部11bは、上記コマンドがサーバ部11へ対するものであった場合には、当該コマンド中のパラメータに応じて、所要のリモートメンテナンスの内部処理を実行し (ST73)、これに対し、それがサーバ部11ではなくルータ部12へ対するものであった場合には、同端末1のルータ設定処理部11cを介して、当該コマンドをルータ部12へ転送して (ST74)、そのコマンド中のパラメータに応じたリモートメンテナンスの内部処理を、当該ルータ部12に実行させる (ST75)。

【0115】そして、所要のリモートメンテナンスの内部処理が、端末1のサーバ部11又はルータ部12において実行されると、同端末1の `http` サーバ部11a

は、上記CGI処理部11bから、上記コマンドに対する「ステータス（正常又はエラーステータス）」を取得し、当該ステータスをパラメータとしたhttpレスポンスを、VPNセッションにより（VPNトンネル7を通じ）、リモートメンテナンス装置6のメンテナンスコマンド処理部端末61に向けて送信する（ST76）。

【0116】そして、リモートメンテナンス装置6のメンテナンスコマンド処理部61は、端末1から送信された上記レスポンスを受信し（ST77）、以上により、このリモートメンテナンス処理を完了する。

【0117】＜リモートメンテナンス終了指示処理＞本リモートメンテナンス終了指示処理は、リモートメンテナンス装置6を使用して、実際にリモートメンテナンスを終了することを保守サーバ3に伝えることを目的とする。以下、図面により、本リモートメンテナンス終了

保守サーバ3のhttpサーバ部31では、リモートメンテナンス装置6から送信された上記コマンドを受信し（ST79）、以下、処理を④のVPNセッション終了指示処理へと受け渡す（図示の記号「E」により連続）。

【0121】なお、本リモートメンテナンス終了指示処理は、実際には、以降に続くVPNセッション終了指示処理が完了するまで起動状態を維持する。その詳細については、以下のVPNセッション開始指示処理で併せて

＜④VPNセッション終了指示処理＞

本VPNセッション終了指示処理は、上述のリモートメンテナンス終了指示処理の内部処理として機能し、リモートメンテナンスの終了指示に引き続き、IPsecセッションを解除することを目的とする。以下、図面により、VPNセッション終了指示処理の詳細を説明する。

【0123】図10は、本発明の方法例に係るVPNセッション終了指示処理を説明するためのフローチャートである（一部、リモートメンテナンス終了指示処理を含む）。

【0124】同図に示すように、本VPNセッション終了指示処理は、上述のリモートメンテナンス終了処理による起動を契機（E）に開始される。即ち、保守サーバ3のVPNゲートウェイ設定処理部33は、まず、端末1のルータ部12をIPsecの対象ホストとした「IPsecセッションの終了設定（VPNゲートウェイ4のtelnetコマンドの実装形態により異なる）」をパラメータとしたtelnetコマンドを、ローカルネットワークセッションにより、VPNゲートウェイ4に向けて送信する（ST80）。

【0125】VPNゲートウェイ4は、その設定コマンド受信処理部42において、保守サーバ3から送信された上記コマンドを受信して（ST81）、当該コマンドをVPN処理部41へ受け渡し、さらに、このVPN処理部41において、端末1のルータ部12との間で確立されているIPsecを相互に終了する処理を実行すると共に（ST82、ST83）、IPsecイニシエ

指示処理の詳細を説明する。

【0118】図9は、本発明の方法例に係るリモートメンテナンス終了指示処理を説明するためのフローチャートである。

【0119】同図に示すように、本リモートメンテナンス終了指示処理は、リモートメンテナンスの実施者の手動操作により開始される。即ち、リモートメンテナンス装置6のメンテナンスコマンド処理部61は、「リモートメンテナンス終了を示すコード」をパラメータとしたhttpコマンドを、ローカルネットワークセッションにより、保守サーバ3のhttpサーバ部31に向け送信する（ST78）。

【0120】

【外3】

20 説明する（図示の記号「F」により連続）。

【0122】

【外4】

30 タ設定を消去して（ST84）、IPsecのリンクを終了する（ST85）。

【0126】次に、以上のIPsecの終了に伴い、VPNゲートウェイ4の設定コマンド受信処理部42は、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとしたtelnetレスポンスを、ローカルネットワークセッションにより、保守サーバ3のVPNゲートウェイ設定処理部33に向けて送信する（ST86）。

40 【0127】そして、保守サーバ3のVPNゲートウェイ設定処理部33は、VPNゲートウェイ4から送信された上記レスポンスを受信し（ST87）、以上により、このVPNセッション終了指示処理を完了して、処理を のリモートメンテナンス終了指示処理へと引き戻す。

50 【0128】ここで、リモートメンテナンス終了指示処理は、上述のVPNセッション終了指示処理における正常又は異常レスポンスの受信を契機（ST87のステップ）に開始される。即ち、保守サーバ3のhttpサーバ部31は、上記レスポンスに対する「ステータス（IPsec確立又はエラーステータス）」をパラメータと

した http レスポンスを、ローカルネットワークセッションにより、リモートメンテナンス装置 6 のメンテナンスコマンド処理部 61 に向けて送信する (ST88)。

【0129】そして、リモートメンテナンス装置 6 のメンテナンスコマンド処理部 61 は、保守サーバ 3 から送信された上記レスポンスを受信し (ST89)、以上により、この VPN セッション終了指示処理を完了する。

【0130】なお、リモートメンテナンス装置 6 の後処理として、保守サーバ 3 から正常な IPsec 確立レスポンスが返送されたら、今回のリモートメンテナンス処理を終了する。

【0131】以上、本発明の実施の形態を、その適用システム構成例及び方法例につき説明したが、本発明は、必ずしも上述した手法にのみ限定されるものではなく、

また、同方法例では、最後に、⑨のリモートメンテナンス終了指示処理、及び⑩の VPN セッション終了指示処理を実行する場合を例に挙げたが、これら各処理は、本発明にとって必須の要件ではなく、場合によっては、これらを省略するようにしてもよい。但し、無意味に VPN セッションを継続させておくことは、端末 1 のセキュリティをいたずらに低下させることに等しいので、これら各処理の実行は、強く推奨されるものである。

#### 【0134】

【発明の効果】以上、詳細に説明したように、本発明によれば、従来は人手が必要とされていた端末のメンテナンスを、インターネットを経由してリモートで実施することが可能となることから、保守稼働の低減、並びに、通信費用や派遣費用などの保守コストの軽減を図ることができる。

【0135】また、従来は、セキュリティレベルの確保のために、リモートメンテナンス用の独自の暗号処理技術等が必要であったが、本発明によれば、下位の IPsec レベルにおいて暗号処理及び認証処理を行うことにより、十分なセキュリティが確保されるため、例えば、ルータメンテナンスのアプリケーションを、端末の内線からの制御と、リモートメンテナンス制御とに共通して利用することなども可能となる。この結果、アプリケーションの開発コスト及び維持コストを、大いに削減することができる。

#### 【図面の簡単な説明】

【図 1】本発明の適用システムであるリモートメンテナンスシステムの構成を示す図である。

【図 2】本発明の方法例に係る設置通知処理を説明するためのフローチャートである。

【図 3】本発明の方法例に係る端末 VPN 鍵設定処理を説明するためのフローチャートである。

【図 4】本発明の方法例に係る故障通知処理を説明するためのフローチャートである。

【図 5】本発明の方法例に係るリモートメンテナンス要求処理及び VPN ゲートウェイ設定処理を説明するため

本発明にいう目的を達成し、後述の効果を有する範囲内において、適宜変更実施することが可能なものである。

【0132】例えば、以上に説明した方法例では、のリモートメンテナンス開始指示処理が、リモートメンテナンスの実施者から手動操作により実行されて初めて、所要の VPN トンネル 7 を確立させる場合を例に挙げたが、これに代え、の VPN ゲートウェイ設定処理の終了後、のリモートメンテナンス開始指示処理を実行することなしに、連続しての VPN セッション開始指示処理を起動、実行させることなども、無論可能である。この場合、端末 1 の故障通知後、連続的に IPsec が確立されることになる (何れの処理を採用するかについては、運用上のポリシーに委ねられる)。

#### 【0133】

#### 【外 5】

のフローチャートである。

【図 6】本発明の方法例に係るリモートメンテナンス開始指示処理を説明するためのフローチャートである。

【図 7】本発明の方法例に係る VPN セッション開始指示処理を説明するためのフローチャートである。

【図 8】本発明の方法例に係るリモートメンテナンス処理を説明するためのフローチャートである。

【図 9】本発明の方法例に係るリモートメンテナンス終了指示処理を説明するためのフローチャートである。

【図 10】本発明の方法例に係る VPN セッション終了指示処理を説明するためのフローチャートである。

#### 【符号の説明】

α…リモートメンテナンスシステム (適用システム)

1…端末

11…サーバ部

11a…http サーバ部

11b…CGI 処理部

11c…ルータ設定処理部

11d…故障検出処理部

11e…コマンド送信処理部

12…ルータ部

2…インターネット

3…保守サーバ

31…http サーバ部

32…CGI 処理部

33…VPN ゲートウェイ設定処理部

4…VPN ゲートウェイ

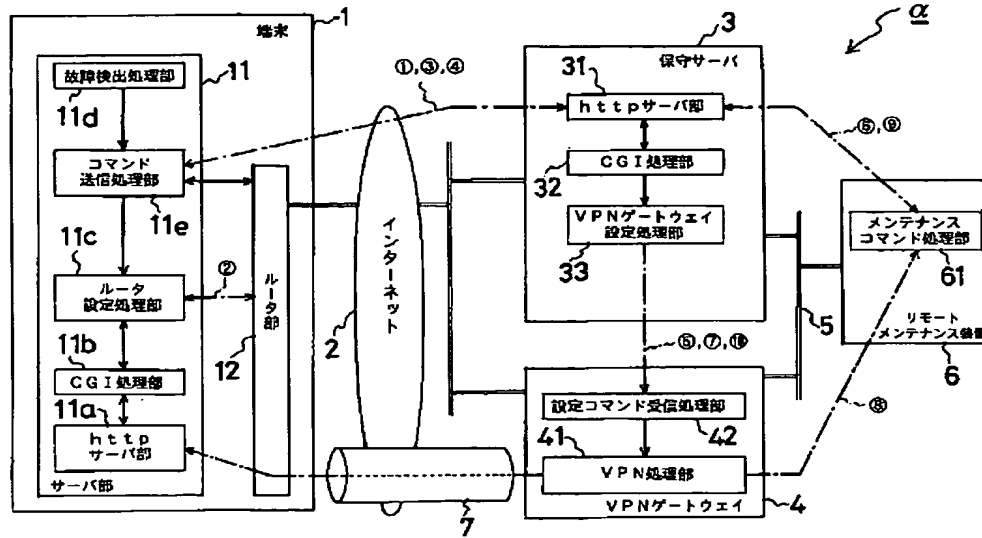
41…VPN 処理部



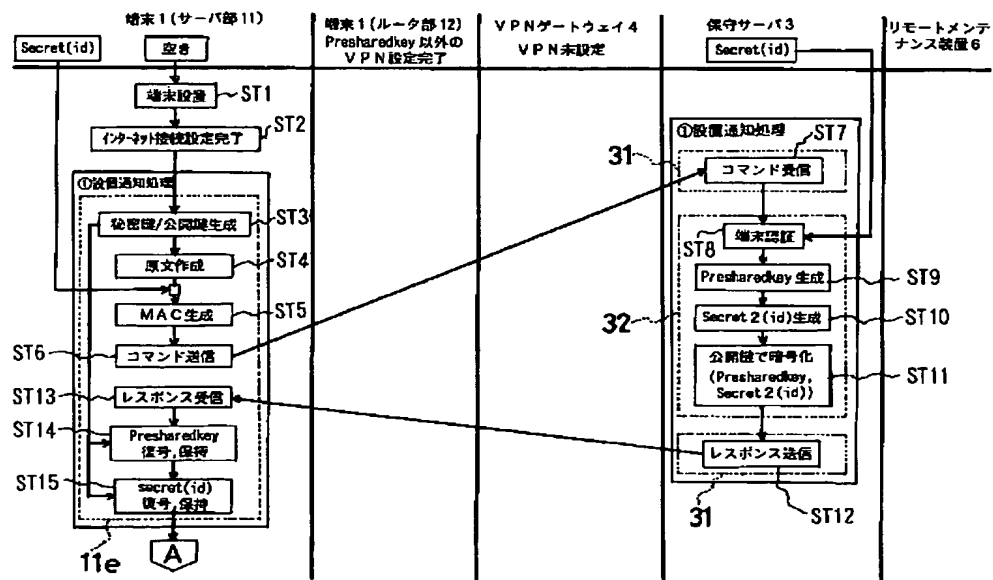
42…設定コマンド受信処理部  
5…ローカルネットワーク  
6…リモートメンテナンス装置

61…メンテナンスコマンド処理部  
7…VPNトンネル

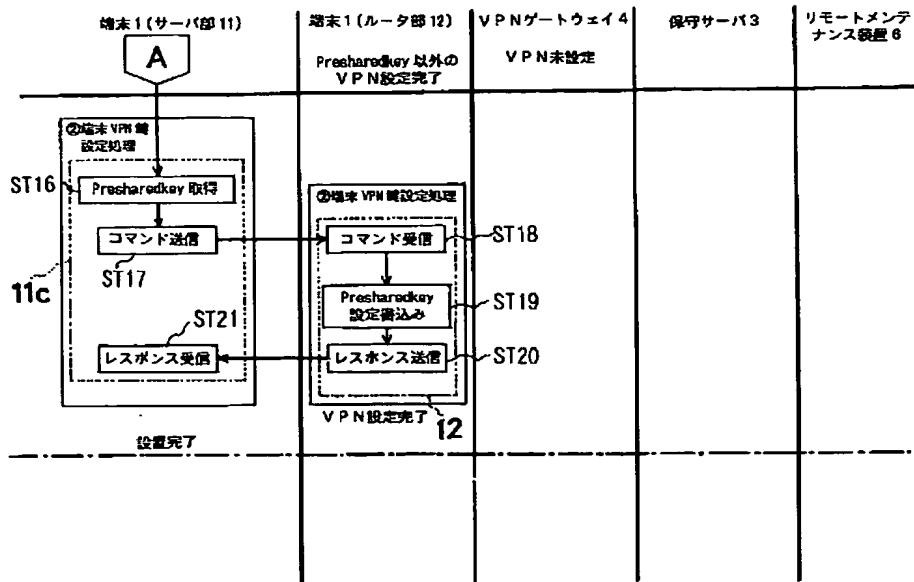
【図1】



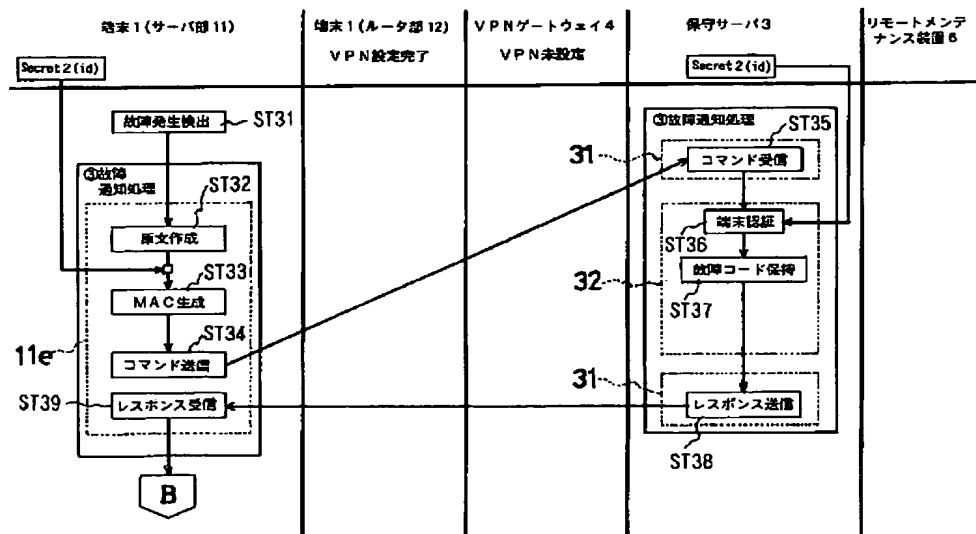
【図2】



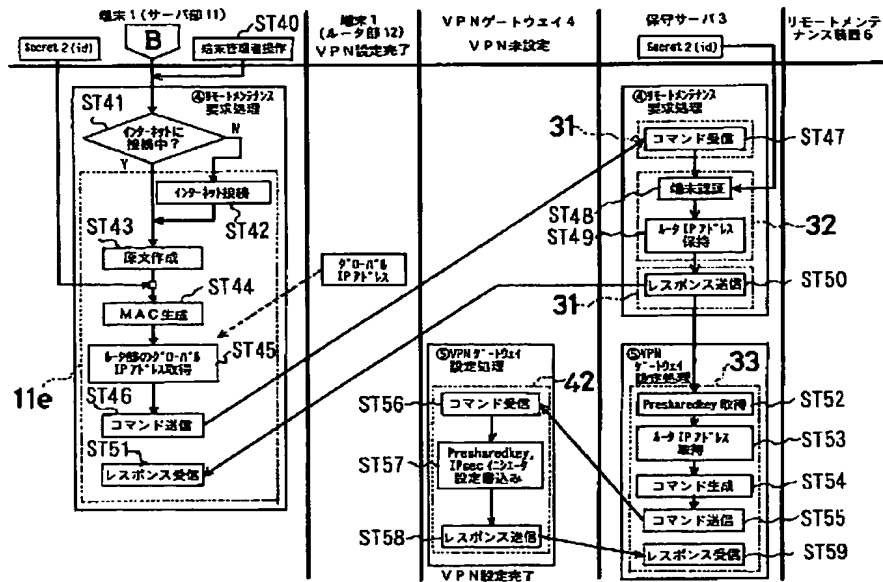
【図3】



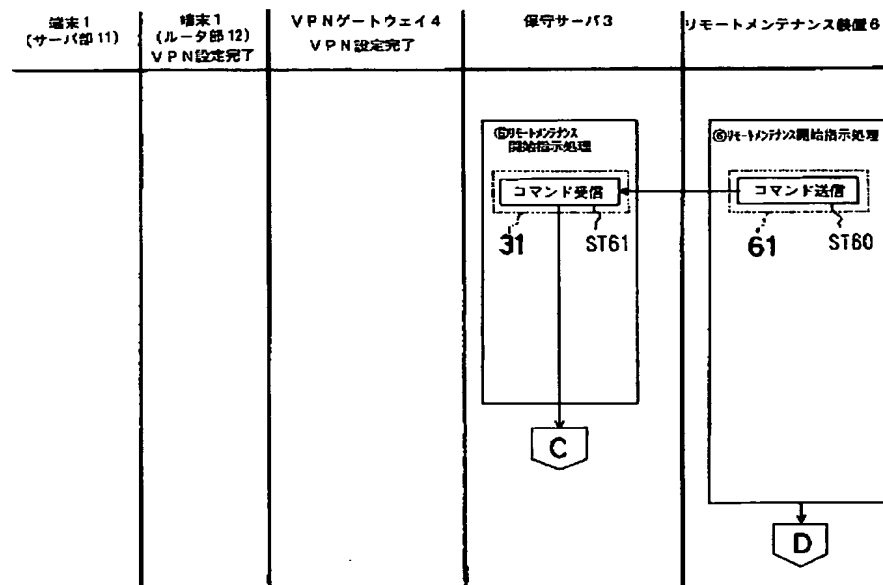
【図4】



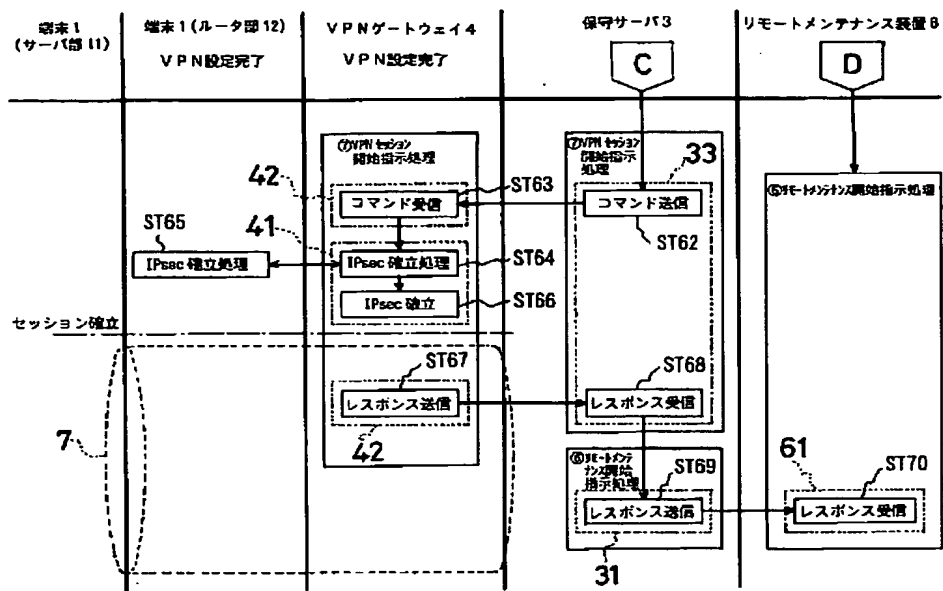
【図5】



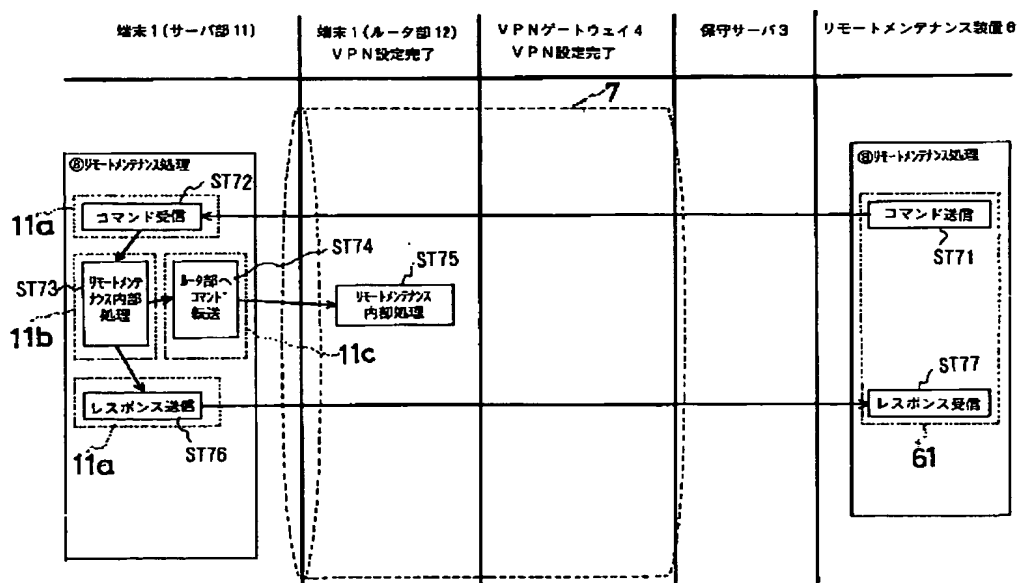
【図6】



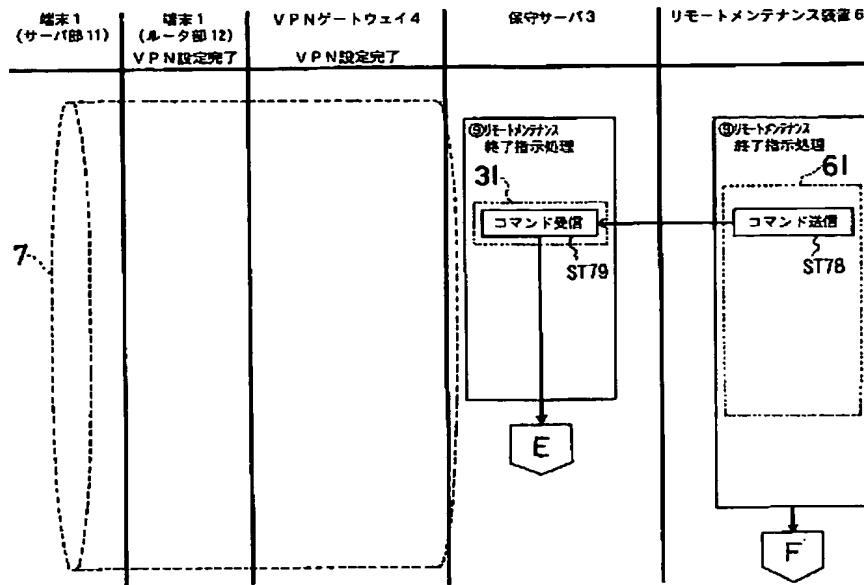
【図7】



【図8】



【図9】



【図10】

